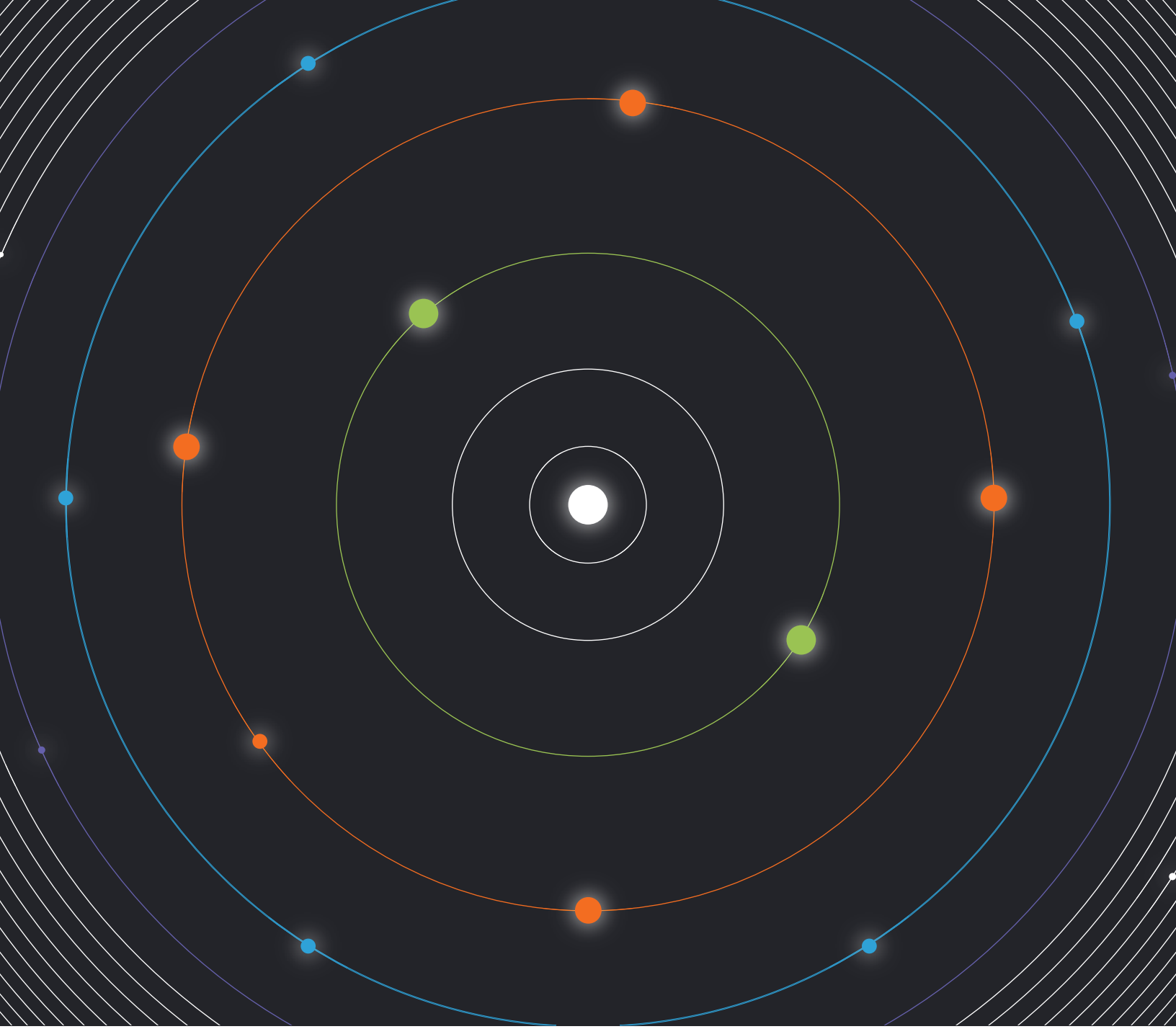

You Can't Secure What You Can't See: Cybersecurity in a Converged IT/OT/IoT Environment

MARKET TRENDS REPORT

govloop Gigamon® ClearShark fierce technology solutions

Executive Summary

Federal agencies have long mitigated risks to industrial control systems by separating or "air-gapping" information technology (IT) and operational technology (OT).

OT systems manage a wide range of industrial control systems that are targets of terrorists and saboteurs. Unlike IT systems developed to safely connect to the outside world, OT systems were designed to operate in a virtual vacuum, making them vulnerable to external threats.

Much of the OT in use today was designed when network connectivity was limited and operational activities were concentrated at a few locations. From the beginning, the isolation of OT was a security feature. Like a person born without an immune system, OT existed and functioned in a bubble.

That bubble is threatening to burst.

As agencies pursue efficiency, OT and IT networks are converging. Ramping up the use of automation and remote monitoring of geographically distributed OT systems increases cyber vulnerability. Deploying Internet of Things (IoT) devices — cameras, thermal imaging systems, thermostats — further increases the security risk to OT systems.

The goal for agencies is to balance the benefits of OT, IoT and IT through convergence and connectivity without compromising the security of infrastructure. For that to happen, agencies must redouble efforts to protect and monitor systems that have unique requirements, limitations, vulnerabilities and security risks. The Biden administration has made that a priority, incorporating OT into the May 12, 2021 executive order on cybersecurity.

To learn more about how agencies can maintain the security of converged systems, GovLoop teamed with ClearShark, an engineering-focused cybersecurity solutions provider; and Gigamon, a technology company with expertise in network visibility and traffic monitoring. This report will discuss how government agencies can use visibility and monitoring tools to neutralize security threats that arise when integrating OT with IT and IoT networks.

"The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT))."

- President Biden's 2021 Executive Order on Improving the Nation's Cybersecurity

By The Numbers

40%

of industrial sites have at least one direct connection to the public internet.

84%

of industrial sites have at least one remotely accessible device.

25%

of asset-centric enterprises will adopt a hybrid model to secure operational technology environments by 2021, up from 10% in 2018.

The Energy Department's Multiyear Plan for Energy Sector Cybersecurity does not fully address risks to the grid's distribution systems, including vulnerabilities associated with internet-accessible industrial control systems devices and networked consumer devices.

– The U.S. Government Accountability Office

"Replacement of OT infrastructure with IT systems is opening new vulnerabilities and risks that are pushing security and risk management leaders to update security approaches and strategies."

– Gartner

90%

of organizations had at least one OT system intrusion in 2020, a 19% increase from 2019, and 65% had three or more intrusions.

78%

of critical infrastructure managers said a successful attack on their organization's industrial control systems (ICS) or supervisory control and data acquisition (SCADA) is at least "somewhat likely" within the next 24 months.

Challenge: New Resiliency, Security and Safety Risks

Most OT systems were deployed originally as "air-gapped" systems, or standalone deployments without any direct connectivity to the outside world. That meant that operators often needed to be physically present to monitor system status, upload new ladder logic to programmable logic controllers (PLCs) or update screens on human machine interfaces (HMIs). Eventually, more sophisticated environments introduced local network connectivity for OT systems.

Even in these scenarios, connectivity was often limited to a workstation that was outside the control zone but connected to a network that was completely isolated from the rest of the enterprise IT infrastructure.

Over time, as critical infrastructure and specialized personnel became more mobile and geographically distributed, several key factors initiated a convergence between OT and IT environments.

Many agencies faced pressure to increase speed and efficiency. Automation of critical functions like monitoring, reporting and data analysis supported this objective, but it required connectivity between OT systems and IT networks to execute.

As enterprise IT management and security practices matured, there was a desire to bring modern IT best practices like asset management and patch management to OT systems. Network connectivity is central to many of these activities as well.

Finally, a new generation of IoT devices emerged that could complement traditional OT functions with more modern capabilities and innovations. For example, the availability of IoT cameras, thermal imaging systems, thermostats and other sensors provided new ways to monitor critical infrastructure systems and initiate more proactive maintenance on ICS.

Unforeseen Consequences

These devices, however, are also dependent on modern IT infrastructure, including, in some cases, managed cloud services that require internet connectivity.

This gradual convergence of OT, IT and IoT systems is helping agencies reduce costs and improve effectiveness through greater agility. It also achieves some security benefits, such as the ability to apply modern cybersecurity tools and techniques to OT. In the process, however, it also introduces new operations and security challenges that must be mitigated.

One problem is that the aging distributed control systems (DCS) and supervisory control and data acquisition systems at the center of many OT environments were not intended to be connected to IT networks. As a result, remote access, visibility and threat analysis were not design priorities.

"The level of processing power that some of these OT devices have can't stand up to network scans," said Andrew Callan, Systems Engineer for ClearShark. "They fall over."

In addition, best practices in IT environments such as vulnerability scanning, patch management and endpoint detection and response often aren't possible with legacy OT systems.

"Some of these systems use such old operating systems, there's not a patch available," said Darshan Shah, Senior Manager for Solutions Marketing at Gigamon. "Endpoint detection is not going to work in those situations, and security falls back to the network."

In addition, there are two other key challenges:

- **Blind spots** with data center and/or cloud visibility that prevent security tools from seeing a complete picture of all network activity. While most network security tools were designed to protect communications based on the TCP/IP protocol, OT networks often utilize specialized protocols. Some of these protocols are proprietary, and even those that are standards-based are not always supported by commercial security products. Even if the necessary protocol support exists in a security product, it may not be practical for the tool to gain visibility into the relevant traffic flows due to constraints of the OT architecture.

- **Escalation of network traffic volumes** to levels that overwhelm the security monitoring and enforcement tools used to protect the environment. Monitoring tools can get overwhelmed by large amounts of duplicate or irrelevant traffic, limiting their accuracy and effectiveness. This makes it difficult to inspect traffic in a timely manner, which puts mission-critical functions at risk.

Without attention, these issues present real-world safety and security risks. Unfortunately, performing the necessary security tool upgrades to keep up with escalating traffic volumes is cost-prohibitive for many budget-constrained agencies.

Solution: A Holistic Approach to IT, OT and IoT Security

A robust visibility and analytics solution provides a scalable and comprehensive platform for ongoing insights into both legacy OT and modern IT networks, along with the ability to deliver optimized traffic feeds to security tools that protect converged IT, OT and IoT environments.

Eliminate Blind Spots

A third-party solution from a reputable vendor will extend visibility across legacy OT infrastructures, modern on-premises data centers and public cloud infrastructure. This includes tapping into the switches carrying data between PLCs and HMIs over ethernet and other methods of observing OT traffic.

In parallel, agencies can deploy containerized software at the edge to capture traffic flowing to the cloud from modern IoT devices. Finally, as the overall volume of east-west traffic grows in primary IT environments, the right solution illuminates this activity, including in virtualized environments where traffic may not reach the physical network directly.

By providing more comprehensive visibility into the converged environment, solutions that stabilize environments created by OT-IoT-IT convergence make it easier to deploy network security tools that mitigate risk to vulnerable and unpatchable systems. A feature of the best solutions is their ability to make collected data more meaningful and actionable by decrypting Transport Layer Security traffic centrally for scalable inspection and filtering traffic to tools with granularity up to Layer 7.

"With OT, IoT and IT convergence, visibility is more critical than ever before," said John Quezada, a Federal Sales Engineer at Gigamon. "You always want to have visibility into what's going on within the environment and be able to monitor it."

Optimize Tool Performance and Costs

In addition to delivering visibility across converged OT, IT and IoT environments, premier solutions also help agencies overcome the performance and scalability challenges mentioned above.

A good solution "offloads a lot of the processes that tools typically have to apply to traffic before they can get to the core mission of analyzing," Quezada said. "A lot of legacy tools are only expecting traffic at a rate of 100 megs or less. One or 10 gigabits per second line rates will be more than these tools can handle."

Integrated traffic de-duplication reduces the amount of unnecessary traffic directed to security monitoring and enforcement tools, often in the range of 40 to 60 percent, preventing packet loss that can result when tools are overloaded – and also avoiding expensive upgrade costs. Many medium-sized organizations have saved millions of dollars in tool upgrades by using traffic reduction techniques like de-deduplication, packet slicing, flow mapping, NetFlow, etc.

Consistent use of smart application filtering culls data with application (Layer 7) granularity; only essential traffic reaches tools – no more than is needed for those to perform critical tasks. For example:

- Lower-risk/higher-volume traffic, such as certain video-streaming applications, can be filtered out by simply selecting by application.
- A security tool that specializes in OT protocol analysis can receive only the relevant traffic data that it can derive insight and value from.
- That same data can be excluded from the traffic data sent to IT-focused security products that aren't capable of analyzing OT protocol traffic.

"Instead of sending multiple copies of packets to the tools and making them inefficient, effective solutions de-duplicate data so that only one copy is routed to the tools at the right speed," said Quezada. "It's much more efficient."

Reducing the burden of processing irrelevant data helps agencies apply the Purdue model and other best practices at scale without interruptions or unnecessary costs.

Scaling the Purdue Model as Traffic Volume Multiplies

Agencies can't talk about cybersecurity in a converged environment without talking about the Purdue model. Purdue is a widely used reference architecture of ICS network segmentation, delineating between distinct levels of ICS equipment. Level one starts with low-level components such as motors, actuators and solenoids, and the model continues to levels four and five, which include mainstream IT systems.

The Purdue Model (see Figure 1 below) strongly recommends implementing network controls such as firewalls between each level of the model, and only allowing traffic that is explicitly required to move between the levels.

The problem is that in a converged environment, the number of connected devices multiplies and the volume of network traffic surges, including some protocols the legacy firewalls will not be able to analyze or effectively apply policy to.

In contrast, but equally as detrimental, modern security tools added to support IT and IoT devices often lack support for legacy OT protocols, such as Modbus and S7, that are often found in ICS environments. Without a standardized approach for providing tool visibility and traffic data optimization – and directing the right traffic types of the right tools – scalability and security effectiveness problems develop.

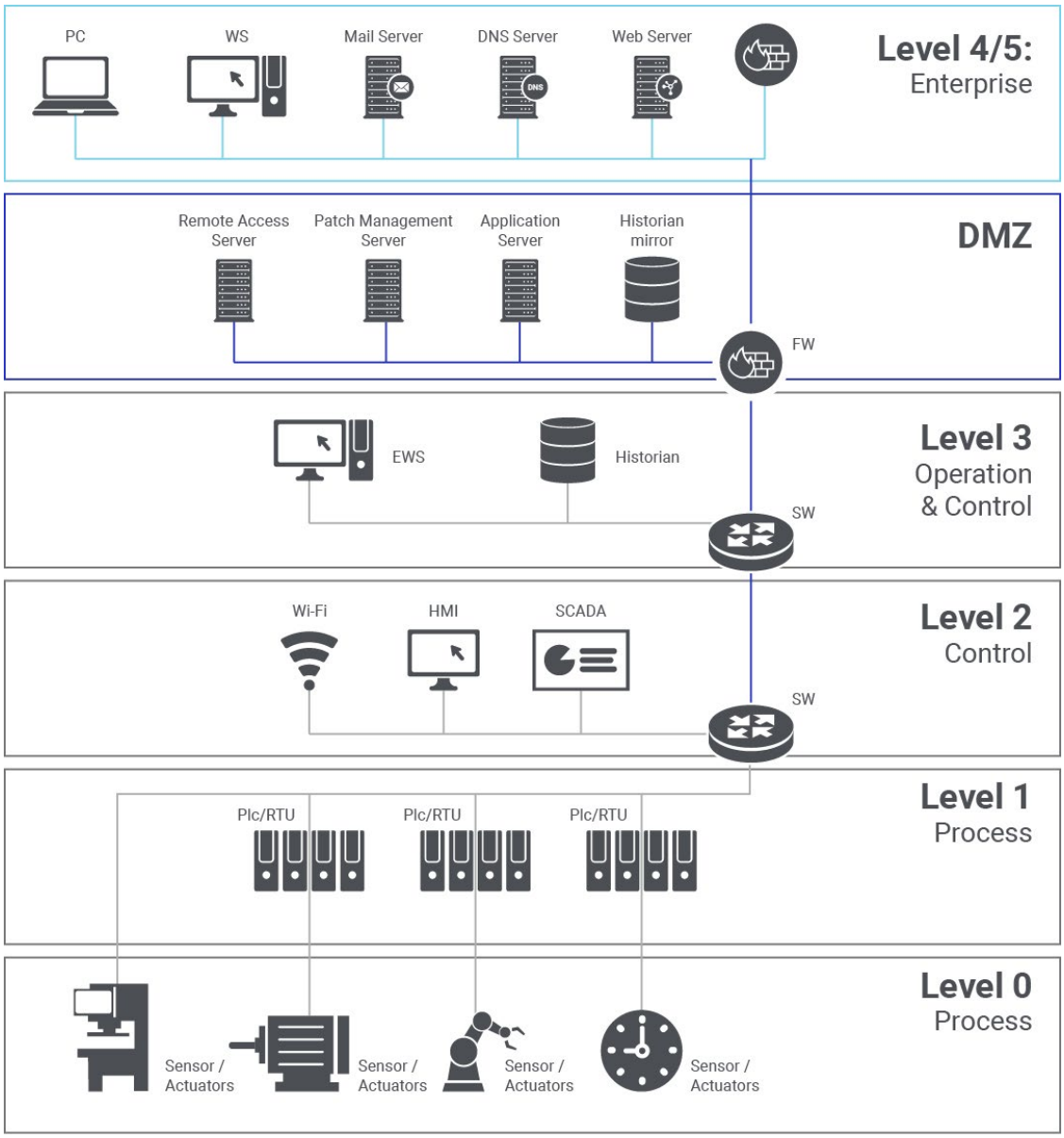

Figure 1. *Purdue Model*

Use Case: Protecting the Water Supply

Consider a typical use case for improving cybersecurity in converged OT-IT-IoT environments. The OT of a critical water treatment plant using a SCADA system that oversees numerous individual distributed control systems. To allow logging data from OT devices such as programmable logic controllers and human-machine interfaces, for example, to be aggregated in an enterprise data platform, network operators establish communication between OT and IT environments. Cameras and thermal imaging systems are deployed to detect fire hazards and electrical faults. The IoT devices are managed in the cloud.

There are three main challenges:

1. Lack of visibility into the OT environment
2. A new requirement to monitor traffic to the cloud
3. New vulnerabilities for the OT system

Solutions to the first and second challenges include tapping into switches carrying data between PLCs and HMIs over ethernet. Deploying containerized software on edge compute devices allows operators to view the industrial IoT and to monitor cloud traffic.

Agencies can address the third concern by efficiently delivering network traffic (whether on-premises or in the cloud) to the correct tools, passively monitoring data packets to identify systems, account for vulnerabilities and address malicious or abnormal traffic.

HOW GIGAMON AND CLEARSHARK HELP

The Gigamon Hawk Visibility and Analytics Fabric, a scalable and comprehensive platform, enables visibility into legacy OT and modern IT networks. It optimizes traffic feeds to security tools that protect converged environments.

Gigamon extends visibility across legacy OT infrastructure, modern on-premises data centers and public cloud infrastructure. Gigamon solutions:

- Tap into switches carrying data between PLCs and HMIs
- Deploy to the edge to capture traffic flowing from IoT devices to the cloud
- Make east-west traffic visible in primary IT environments
- Ease deployment of network security tools and mitigate systems' risk
- Make collected data meaningful and actionable, decrypting TLS traffic centrally for scalable inspection and filtering traffic to tools with granularity up to Layer 7

Gigamon Hawk Visibility and Analytics Fabric helps agencies overcome performance and scalability challenges by:

- Integrating traffic de-duplication and reducing unnecessary traffic to security monitoring and enforcement tools
- Load balancing and providing flexible ports that can seemlessly match network traffic speed to the processing rate of tools
- Partitioning traffic not needed for a tool to function

"The goal is making sure that security and network tools have the right visibility into parts of the network so the tools can easily analyze them," Quezada said.

ClearShark's highly-trained team of solutions architects and deployment engineers are ready to partner with government customers to design and deploy OT Security capabilities. ClearShark works exclusively with government customers, with a strong emphasis on projects in high-side environments. ClearShark's approach to monitoring, analytics, and automation emphasizes Gigamon's technologies.

For more information on Gigamon solutions for OT/ICS/IoT, visit https://www.gigamon.com/solutions/industry/IOT.html

Conclusion

OT environments designed to operate in isolation have become more vulnerable to attack than ever.

Fueling the vulnerability is the convergence of OT, IT and IoT, which also has benefits. Using external, remotely controlled monitoring devices, for example, has improved many aspects of OT environments, while also making them more vulnerable to attacks that OT architecture can't easily repel.

The only way to securely unlock the benefits of convergence is through complete and consistent visibility across all legacy OT and modern IT environments. Gigamon and ClearShark make this possible by:

- Extending visibility to the entire infrastructure, including east-west traffic and other blind spots
- Making traffic data more actionable through Layer 7 granularity and techniques such as centralized TLS decryption
- Optimizing the performance, scalability and cost of security tools by sending them only relevant traffic

"With the IT-OT-IoT convergence, visibility is more critical than ever before," said Quezada. "You always want to have visibility into what's going on within the environment and be able to monitor it."

ABOUT GIGAMON

Gigamon is the first company to deliver unified network visibility and analytics on all data in transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate. Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 4,000 organizations, including 80 percent of the Fortune 100 and hundreds of government and educational organizations worldwide. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit gigamon.com.

ABOUT CLEARSHARK

ClearShark is an IT Solutions Provider with a first-class engineering team, comprised of mission-focused, results driven SMEs from the IC, DOD, and Civilian government. We are focused and innovative, priding ourselves in our lean line card, making investments in technologies we believe in, and being free to pivot and find disruptive technologies.

Learn more at https://www.clearshark.com/

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop